TOP SECRET "U"

TICOM/I-84

FURTHER INTERROGATION OF

R. R. DR. HUETTENHAIN AND SDF. DR. FRICKE

OF OKW/CHI

Attached is a report of further interrogation of Huettenhain and Fricke at CSDIC (UK), Camp 2, on 25th August, 1945.

The interrogation was largely based on a series of questions framed by Mr. W. F. Friedman which were put by Major Seaman. The answers were subsequently discussed with Mr. Friedman.

TICOM
4 Sept. 1945

Copy No. 17
No. of pages 7

DISTRIBUTION

British
1. Director
2. D.D.3
3. D.D.4
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt. Col. Leathem
10. Major Morgan

U.S.
25-26. OF 20-G (2) (via Lt. Pendergrass)
27. G-2 (via Lt.Col.Hillea)
28-29. S.S.A. (2)(via Major Seaman)
30. Director, S.I.D. USFET (via Lt.Col.Johnson)
31. Lt.Col.Lewis Powell
34 MR FRIEDMAN

TICOM
11. Chairman
12-13. S.A.C. (2)
14. Cdr. Bacon
15. Cdr. Mackenzie
16. Cdr. Tandy
17. Lt. Col. Johnson
18. Lt. Cdr. Manson
19. Major Seaman
20. Lt. Vance
21. Capt. Cowan
22. Lt. Fehl
23-24. Ticom Files (2)

Additional
32. Mr. Twinn
33. S.A.C. for Capt. Ginsburg (Personal)

Approved for Release by NSA on 07-25-2017, FOIA Case # {66109}

Return to the NSA Technical Library when no longer needed
S-45884
Copy No.

Doc ID: 6587329

Present: Cdr. DUDLEY-SMITH. R.N.
Major SEAMAN. AUS.
Lt.Cdr. FORSTER. RNVR.
Capt. GINSBURG. I.C.

1. Who made and wired the Enigma wheels, and where was this done?

The patents were held by the firm of HEIMSOETH & RINCKE, but they did not build the machines. Heimsoeth was a lawyer from Cologne and Rincke a woman. The man who developed the machine, in collaboration with Fenner, was Dipl Ing ((Willi)) KORN. The firm received a royalty on every machine built and the army tried to get rid of them. They were located in Berlin on UHLANSTRASSE. The wheels for the army and air were made by KONSKY & KRUEGER, Berlin CHAUSSEESTRASSE, a small firm which probably made only enigma machines. The naval machines were made by ERTEL in Munich. Other machines were made by the OLYMPIA typewriter company in ERFURT, who also made Lueckenfuellerwalze.

2. What became of the various cryptanalytic machines which OKW/Chi had made for their aid in research?

They were moved from Berlin to Halle, where they were in use, and then they were taken south, probably to CHIEMSEE. The location of those built for OKL is uhknown.

3. What were the X^2 and W^2 methods referred to by another PW?

W^2 was not familiar to them. X^2 had to do with the separation of Hagelin messages written on a width into two classes of columns. We asked which particular form of test was used. They said they used various methods and tried to refine them. It amounted to a sharper application of Gauss' laws, which would be found in Von Mises' "Kollektiv". They did not recall the exact refinements as Herr Dr SCHULZE worked on them at OKW and Reg Baurat MARQUARDT at OKH. The latter wrote a paper on it but Fricke never read it. Huettenhain considered it unlikely that a refined mathematical method would succeed if the crude X^2 test fails. Gauss' formulae always suffied if the material is workable at all, and no finer method is needed. Fricke pointed out that the same thing was true, in his experience, in curve-fitting for scientific purposes, where Gauss' formulae always suffice and no finer method is needed. He had done no recent work on the subject.

4. What could they tell us about the Chi conferences in Berlin held at the instigation of General Gimmler in Autumn 1944?

When Gimmler took over Ag/WNV he started these talks in order to put forth his views. He gave a sort of standard lecture to various groups at various times. His approach was that of the officer-layman. He had no technical knowledge and no one could tell him any thing. His speech began something like this: "I will make Chi an orderly organisation. Before this, it has not been so. We must have three pillars in our work: Development, Security, and Cryptanalysis ". Then he would expound his views on the relations between these three. The head of the first branch must be an Officer, who would know what the troops need. The second could be left to a civil servant. It is the most important of the three, and the other two exist primarily to fertilize it. He considered cryptanalysis very unimportant in itself. Gimmler once asked Fenner what he thought of this view. Fenner replied that he would not care to say. We asked what Kettler and Mettig thought about it.

Doc ID: 6587329

They thought they had no views. Did OKW/Chi receive any directives from above as to what they were to work on? To some extent. Fenner used to mention sometimes that he had been told to emphasize something. But the direction always came too late and was given people who could not seem to realize that systems could not be broken on a day's notice. Directives came probably from WFSt (Wehrmachtfuehrungsstab) to Jodl to Kettler. Before 20 July Kempf (later Kettler) used to go to Canaris, and later Hansen (the heads of the Abwehr) for liaison and briefing about once a week. Kettler never went to see SCHELLENBERG or anyone at the Abw after 20 July. They thought that the Abwehr did not give directives but only briefing on the diplomatic material. They had no information on the control of effort against service systems.

5. What do they know about the M-40 designed by Menzer?

((They described a non-sending model of the captured P-153 and agreed to write up what they knew about it)). It was never used. Only three models were made.

6. What do they know about the Croatian Enigma?

It was commercial type with different wiring, and no stecker. It was probably used both for diplomatic and service traffic. It was worked on and solved at In 7/VI by MARQUARDT in the mathematical section, about two years ago. How were the wheel-wirings obtained? They got them ffom KONSKY & KRUEGER, who did the wiring. They could always get any special wheel wirings from them except the Swiss (who did their own wiring) and the Hungarian. The Hungarians were connected with the firm, and they used to take the wheels at night when the women had gone home and change the wirings enough to make the records useless. How many special wirings did K&K make ? About 200. Special wirings were controlled by Fu, who had records of them all. At one time they brought them all to Huettenhain, who did not want them and passed them to Mettig, who gave them to Oblt ECKER (liaison Officer to OKL/Chi). Whose special wirings were these? They were used by special units of the Army, such as Hitler's train. , KORN said they were getting their records in order and had to keep them somewhere. The officer at Fu connected with this control was Inspektor Boligh, under Colonel FUCHS. It was thought that his office moved to BRESLAU or TORGAU.

7. Did RSHA have its own cryptanalytic bureau?

They did not know of any. General THIELE had said in July or August 1944 that they had no interest in the subject. But they may have had later. Huettenhain thinks they had no organisation but they may have had some embryonic plans for one. He would have heard about it if it had happened. Oblt Adler, head of OKW/Chi Japanese Referat, once said he thought that RSHA had someone working on Japanese cryptanalysis.

8. Did he use uniform training literature in his course at OKW/Chi?

No. The available literature was more or less bad, and the materials he used varied. He tried to use genuine material but usually it was not suitable because it introduced extraneous considerations. The course itself was fixed in its curriculum. He would write up a syllabus showing the subjects covered, time spent on each, number of students, and other details.

9. Where were the projected cryptanalytic devices described im I-37 being developed and by whom?

At OKW/Chi by Dr. ROTSCHEIDT.

Doc ID: 6587329

~~TOP SECRET "U"~~ TICOM/I-84.

10. Does he know to what allied traffic the covername INNSBRUCK applied?

No. (Comdr Dudley-Smith) What was the significance of terms like E30? E is for England, 30 is a serial system number. Similarly AM 10 stood for the American strip system and AM 8 for the enciphered Brown code.

11. What could they tell about the Army-Air-Naval co-ordinating committee on their own code and cipher production and usage?

There was no committee. Each organization did its own testing. They were under no obligation to submit their systems to OKW. The commanders-inchief of the army, air and navy were separately responsible for them Did they get together for discussion? Thiele and Gimmler tried to set up and foster such a group, but it had no sanction from above. Huettenhain was its chairman. The other services were not always represented by the same persons, but usually it was Kapt SINGER for the navy, Haupt PORTH for the air force, and PIETSCH or DOERING for the army. The Foreign Office and Forschungsamt were invited to attend as guests.

The Foreign Office usually sent Hauthal or Schauffler. The Forschungsamt was usually not represented, as they had moved to Breslau. Their representative was Regrat KROEGER. The group met eight or ten times, at intervals of ten days to two weeks. They reported to each other the results of security studies on all German systems and discussed regulations. In theory all systems were to be covered but in fact it was only service systems. They did not always come to any common agreement. For example, the army might wish to reduce the minimum length of a Raster message from 60 to 45 letters and would do so. The air force would say they had no occasion to send such short messages and would keep the old minimum. Another time, they decided that special units using unsteckered Enigma should either encipher the message twice or perform a transposition on it prior to machine encipherment. The Reichsbahn chose the latter method. Menzer represented these other organizations when their security was under discussion. It was emphasized that the meetings were not always attended by the same people. Again, they discussed emergency keys for Raster, Enigma, and so on. Recommendations were made, but there was no obligation to comply. The army usually did, and the air force gave little difficulty, but the navy never complied.

12. What can they tell about the Austrian cryptanalytic bureau: its organization, main personnel, successes, when started work, what became of personnel and records after Anschluss?

They agreed to write up what they knew about this. SIEFFERT was the head of the bureau, and came to work with them. Also there were Dr. MAULER, Dr. LOCKER, and ORR BAILOVIC.

13. Kettler said they were slightly concerned with the development of cyphers for German commercial firms. Can they amplify this?

An Abwehr office, whose designation they could not recall (possibly III-F), did this work for overseas firms. Major MEISSNER had charge of it. When they had difficulty, Oberinspektor MENZER of OKW/Chi sometimes helped. One of the firms was Continental of Hanover. He did not recall what system they used, but Huettenhain had advised that when there was little traffic they should use a one-time pad on a commercial book, such as ABC Code or Mosse.

Doc ID: 6587329

14. Why did he consider Japanese systems bad? What systems specifically?

The attache systems had not been solved (he implied that therefore they were good), nor had something called KOSHI and another that began GAIMU... The systems he considered poor were the transposition ((Fuji)) and a line-transposition of width 19. He undertook to write up the work on Japanese systems which he could remember, and the opinions he had of the systems. On these systems they had good liaison with the foreign office.

15. We described the P-153 captured machine, and asked what they knew about it.

They said it was a version of the M-40 referred to above, adapted for automatic Morse sending.

16. In I-2 Huettenhain said, referring to the American strip system, that after January 1944 only certain lines of traffic could be read, e.g. Berne-London. Why was this possible?

Because they were still using the old systems. What type of strip traffic was read? Was it all diplomatic? At this point Huettenhain began to describe a chart they kept of traffic solved by links and date, which was largely filled but had some holes in it. He apparently thought we had asked whether they broke all of the diplo traffic. When the question was rephrased he said OKH read military strip and OKM naval, while OKW worked only on diplo. Did they break any attache? He did not know; he thought some had been broken, but he did not have anything to do with it. He thought only Cairo attache traffic had been broken, at one particular time, during Rommel's campaign. Did they have any strip captures? No. He was sure the work was entirely cryptanalytic because Kaempf had ordered the section to break before a certain Sunday. In fact this was done and they were always afraid after that that he would expect systems to be broken to order. Did they break any strip referring to clandestine activity? No.

17. What can they tell about the VNs ((decode translation bulletins))?

a. How did they number them? Serially within each month, plus indication of cable or radio origin.

b. Did they indicate the cryptographic system involved? Only in handwriting on the Chi copy. The source was not shown on any of the other copies.

c. How many copies were made and distributed and to whom? The number changed from time to time. For a long time there were 13 typed copies. Later the number was increased and they were stencilled. He does not know to whom they were sent. Did he have a set? No. The language sections got the ones they had produced and von Kalckstein had a complete set, probably.

d. What rules were to be followed in handling them? Were they to be returned to OKW/Chi by the recipients? No, they were kept. They were probably treated like any Geheime Kommandosache.

e. Did they indicate the security classification of the original message: Yes, when shown. For example, 'Strictly Confidential', which appeared on many US State Dept messages, was always indicated.

Doc ID: 6587329

f. How did they indicate garbles and missing groups? By underlining with dots. For missing groups they had to state how many. Linguistic difficulties were indicated by being placed in parentheses and followed by a question mark.

g. Did they make any comments of their own on the VNs? No. What special studies were issued by OKW/Chi based upon VNs? None. They did no intelligence work.

h. Were the translations literal or paraphrased? They were somewhat free translations but not excessively so. When a translation had to depart very much from the original in order to convey the correct meaning, the literal translation was placed in brackets. The Auswärtiges Amt published their decodes in the original language with summaries in German.

i. Dates shown were date of message and date of publication only. If there was delay, a note said 'publication delayed'.

j. Was there a distribution to the research personnel so as to keep them in the picture and provide them with cribs? Research had a right to see them all, but usually just got together with the language sections for this purpose. Search for cribs was made by the registrar of each language section, who kept the log books for the traffic of that section.

18. They knew nothing of the "big American machine".

No studies were made of any USA traffic supposed to be in machine, other than M-209, except voice scramblers. ((See below)).

19. They never heard of any American cipher teleprinter traffic.

20. What other American non-morse traffic or radio "noises" were investigated?

None, except for London-Washington low-grade speech encipherment. This was intercepted by OKW/Chi Gruppe VI at LUDWIGSFELDE about 30 km south of Berlin near Halle. The conversations were of a political nature, and sometimes involved Churchill and Roosevelt as speakers. This traffic was deciphered to the end of the war. Huettenhain thought Telefunken was associated in the construction of the apparatus before the war and hence knew the details. Were the results promulgated as VNs? No, as Chi-Nachrichten. The conversations were not secret. When they were about to get onto something secret, the operator would warn them. The intercept apparatus was developed by LOTZE at Waprüf 7.

21. What knowledge did they have of American or British cryptanalytic agencies?

None whatever. Was there no PW information? One PW in North Africa had said the US and British operated with a very large joint 'park' of Hollerith machinery, but this interrogation was never followed up. No personalities whatever were known. What did they know of the agencies of other countries with whom they did not have liaison? Fenner once talked about the following at a Gimmler conference: Italy, Czechoslovakia, Hungary and Rumania, but they did not recall the details. Nothing known about Sweden, Spain, or Finland. Hayashi was the only Jap man they knew. There had been no information obtained from agents.

Doc ID: 6587329

The following questions received from SSA were put:

22. Huettenhain undertook to write up the methods used in solving the Polish subtractor stencil. He did not know of any Czech one-time-pad such as the one found in the Burg material. He knew of a Polish one which was typewritten, and in which upon investigation no characteristics were found.

23. He could not recall the details of any French military attache systems ((it was considered inadvisable to ask a more specific question)).

24. He did not know of any exchange of weather information with the Japs. Did he know of any joint-use systems for Jap-German communication? Enigmas were given to the Japs, without stecker. He does not know where they were used, but thinks they were for naval use in the Far East. When unsteckered enigma was found to be readable, it was recommended to Fellgiebel that the Japs should have steckered machines. Fellgiebel vacillated on the decision, and Huettenhain does not know whether it was ever done.

25. They did not try to read Jap weather ciphers, nor did the Reichswetterdienst. Did the latter have a cryptanalytic unit? Yes, under Oberinspektor NAUMANN, in GLINDOW, Potsdam. There were about 10 Inspektoren and 20 to 30 helpers. Naumann had been before the war a merchant from Frankfurt-am-Main. He got his job through Regrat Dr. WUESTHOFF, who was in the office of the Chef Wetterdienst. What was Naumann's ability? He was diligent, had a flair, and was lucky. Most of the staff were meteorologists, as a knowledge of weather was most useful. They worked on Russian, English and Mediterranean weather. Huettenhain's impression is that the Russian was always read. The English was not read after it changed (date unknown). A selected sample (20 to 30 pages) from one day's traffic on the new system was brought to Huettenhain and he was able to determine the system roughly but could not read it. He thought it was additive plus transposition (I believe he meant additive read off through a grille). He did not recall the traffic prefix. No work was done on USA weather. Naumann was not under Voegele. Did Naumann continue to try to break British weather? Huettenhain lent him the use of his machines and said they should try a batch of several days' traffic, during which there was known to be constant weather. He does not know what the result was. The machine used was the Bigramsuchgeraet, previously mentioned.